



decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-132459

(P2000-132459A)

(43) 公開日 平成12年5月12日 (2000.5.12)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード* (参考)
G 0 6 F 12/14	3 1 0	G 0 6 F 12/14	3 1 0 Z 5 B 0 1 7
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B 5 D 0 4 4
	6 6 0		6 6 0 D 5 J 1 0 4
G 1 1 B 20/10		G 1 1 B 20/10	H

審査請求 未請求 請求項の数 7 O L (全 9 頁)

(21) 出願番号 特願平10-304109  
 (22) 出願日 平成10年10月26日 (1998. 10. 26)

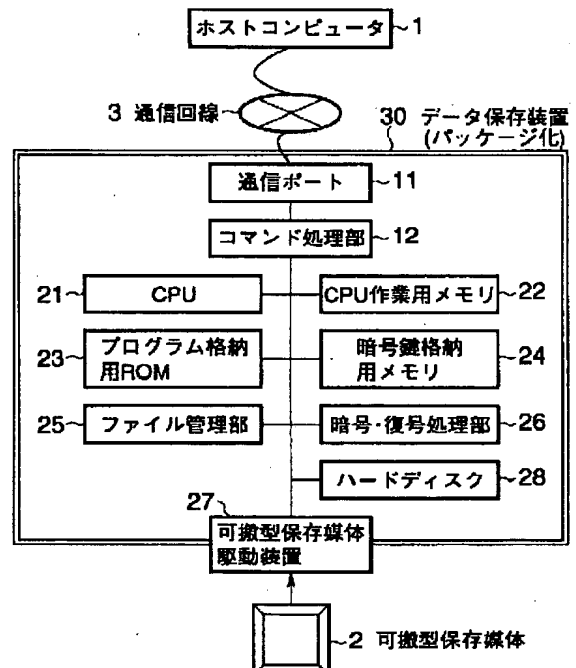
(71) 出願人 000000376  
 オリンパス光学工業株式会社  
 東京都渋谷区幡ヶ谷 2 丁目43番 2 号  
 (72) 発明者 近藤 隆  
 東京都渋谷区幡ヶ谷 2 丁目43番 2 号 オリ  
 ンパス光学工業株式会社内  
 (74) 代理人 100058479  
 弁理士 鈴江 武彦 (外 4 名)  
 F ターム (参考) 5B017 AA06 AA07 BA05 BA07 BA08  
 BA09 BB07 CA07 CA09 CA12  
 CA14 CA16  
 5D044 AB05 DE48 DE49 DE52 GK17  
 5J104 AA09 LA06 PA07

(54) 【発明の名称】 データ保存システム

(57) 【要約】

【課題】 汎用の保存媒体上に格納されたデータファイル  
 に対して消去や差し替えを含む改竄がなされたことを検  
 知できるデータ保存システムを提供する。

【解決手段】 データ保存装置 30 に固有の秘密情報と保  
 存すべきデータとを用いて所定の処理を行なって保存す  
 べきデータの電子署名 102 を生成し、保存すべきデー  
 タと電子署名 102 とを対応させて可搬型保存媒体 2 に  
 記録し、可搬型保存媒体 2 に予め記録された媒体管理用  
 データファイル 103 に、電子署名 102 を、保存すべ  
 きデータのファイルを識別する情報と対応させてレコー  
 ド 105 として記録し、格納されている秘密情報と媒体  
 管理用データファイル 103 を用いて所定の処理を行う  
 ことにより、媒体管理用データファイル 103 の電子署  
 名 104 を生成し、この電子署名 104 と媒体管理用デ  
 ータファイル 103 とを対応させて、可搬型保存媒体 2  
 上に記録する。



## 【特許請求の範囲】

【請求項 1】 ファイル管理機能を用いて保存媒体に対してデータの保存、削除等を行なうデータ保存装置を備えたデータ保存システムであって、前記データ保存装置に固有の秘密情報を格納する格納手段と、

この格納手段に格納された秘密情報と、保存すべきデータとを用いて所定の処理を行うことにより前記保存すべきデータの改竄防止用データを生成する生成手段と、

前記保存すべきデータと前記改竄防止用データとを対応させて前記保存媒体に記録する第 1 の記録手段と、

前記保存媒体に予め記録されている媒体管理用データファイルに、前記改竄防止用データを、前記保存すべきデータのファイルを識別する情報と対応させて記録する第 2 の記録手段と、

前記格納手段に格納されている秘密情報と、前記媒体管理用データファイルを用いて所定の処理を行うことにより、前記媒体管理用データファイルの改竄防止用データを生成し、この改竄防止用データと前記媒体管理用データファイルとを対応させて、前記保存媒体に記録する第 3 の記録手段と、

を具備することを特徴とするデータ保存システム。

【請求項 2】 前記媒体管理用データファイルには、前記保存媒体上に記録されている複数のデータファイルの改竄防止用データを、各々ファイルを識別する情報と対応させて記録することを特徴とする請求項 1 記載のデータ保存システム。

【請求項 3】 前記格納手段は改竄検知用情報を格納しており、この改竄検知用情報と、前記保存媒体に記録されている媒体管理用データファイルと、前記媒体管理用データファイルの改竄防止用データとを用いて所定の処理を行うことによって、前記媒体管理用データファイルが改竄されているか否かを検知する第 1 の検知手段と、前記媒体管理用データファイルに登録されているファイルが全て、前記保存媒体上に存在しているか否かを確認する確認手段と、

前記媒体管理用データファイルのレコードに登録されているデータファイルの改竄防止用データと、保存媒体上に前記データファイルと対応させて記録されている前記データファイルの改竄防止用データとが一致するかどうかを検知する第 2 の検知手段と、

前記格納手段に格納されている改竄検知用情報と、前記保存媒体に保存された前記保存すべきデータと、対応する前記改竄防止用データとを用いて所定の処理を行うことによって、前記保存すべきデータが改竄されているか否かを検知する第 3 の検知手段と、を具備することを特徴とする請求項 2 記載のデータ保存システム。

【請求項 4】 前記保存すべきデータは、通信回線を介して外部装置から送られてきたデータか、あるいは、前記データ保存装置のデータ入力機能を用いて入力された

データであることを特徴とする請求項 1～3 のいずれか 1 つに記載のデータ保存システム。

【請求項 5】 前記保存媒体を初期化する時、あるいは初めてファイルを記録するときに、前記媒体管理用データファイルを前記保存媒体に記録する手段を有することを特徴とする請求項 3 または 4 記載のデータ保存システム。

【請求項 6】 前記ファイル管理機能は、前記保存媒体上のデータファイルを削除する時に、前記媒体管理用データファイルから消去するデータファイルのレコードも削除する機能を持つことを特徴とする請求項 3 または 4 記載のデータ保存システム。

【請求項 7】 前記保存媒体は、前記データ保存装置に着脱自在な可搬型保存媒体か、あるいは、前記データ保存装置内に配置された固定型保存媒体であることを特徴とする請求項 1～6 のいずれか 1 つに記載のデータ保存システム。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はデータ保存システムに関するものである。

【0002】

【従来の技術】例えば光磁気ディスクや CD-R、DVD、DAT 等の可搬型保存媒体に、テキストファイルや画像ファイル等のデジタルデータを保存した場合には、悪意あるユーザが、当該デジタルデータを全く形跡を残すことなく改竄したり、不正に他のファイルと差し替えたり、不正に消去することが可能である。

【0003】データの改竄検知に関しては、保存するデータファイルに電子署名を付ける方法が一般的である（例えば、特開平 7-221751 号公報や特開平 7-131449 号公報等）。電子署名法は暗号技術を用いた方法であり、基本的にはデータに公知の処理を施してあるコードを抽出し、そのコードを本人しか知らない暗号鍵を用いて暗号化したものを改竄防止用のコード（電子署名）として、オリジナルのデータファイルに対応させて保存することからなる。改竄の有無を検知するには、まず、検知するデータに上記の公知の処理を施してコード 1 を抽出する。また、電子署名データを復号用の鍵を用いて復号してコード 2 を取り出す。その後、コード 1 とコード 2 を比較することで、両者が一致した場合には改竄がなかった、一致しない場合は改竄があったことがわかる。

【0004】電子署名を用いる通常の方法では、データファイル作成者以外の第 3 者がデータ内容を改竄するとそれを検知することができる。しかし、この方法では、データファイル作成者はいつでもデータから電子署名を作成できるため、本物の書類作成後、何時でもデータファイルを作成しなおし、自分しか知らない暗号鍵を用いて、そのデータファイルがあたかも本物であるかのよう

に、電子署名を付与することが可能である。例えば、3年前に作成した公文書（デジタルデータ）の内容を、時間を3年遅らせたPCを用いて改竄し、自分しか知らない暗号鍵を用いて電子署名を付与することで、あたかも3年前に作成した公文書で内容は3年前から改竄されていないように見せかけることができてしまう。問題となるのは、改竄防止用のコードである電子署名を作成する手段（暗号鍵）を、ユーザが自由に使用できるという点である。

【0005】上記のような問題を克服するためには、データファイルの改竄防止用コード作成のための暗号鍵を、ユーザではなく、ハードウェア及びソフトウェア的に安全性が確保されたデータ保存装置が管理し、改竄防止コードはユーザが自由に作成できないようにすることで実現できる。

#### 【0006】

【発明が解決しようとする課題】しかし、上記の方法を用いた場合でも、可搬型保存媒体からデータファイルを消去するという改竄は検知することができない。また、ユーザが上記のデータ保存装置を用いて不正に作成したデータファイルと本物のデータファイルを差し替えるという改竄も検知することができない。つまり、データ作成時に予め本物のデータファイルと偽りの内容を記録している偽物のデータファイルとを上記データ保存装置で作成し、それぞれ別の可搬型保存媒体1、2上に同名のファイルで格納する（この場合、第3者は、偽物を格納した可搬型保存媒体の存在を知らない）。どちらも、データ保存装置の電子署名を持っており、データファイルとしては改竄されていないことが示される。その後、汎用のPCなどを用いて、可搬型保存媒体2上の偽物のデータファイルを、可搬型保存媒体1上の本物のデータファイルに上書きすることで、データファイルを不正の痕跡を残さずに差し替えることができてしまう。

【0007】本発明は、このような課題に着目してなされたものであり、その目的とするところは、汎用の保存媒体上に格納するデータファイルに対して、上述したような消去や差し替えを含む改竄がなされたことを検知できるデータ保存システムを提供することを目的とする。

#### 【0008】

【課題を解決するための手段】上記の目的を達成するために、第1の発明は、ファイル管理機能を用いて保存媒体に対してデータの保存、削除等を行なうデータ保存装置を備えたデータ保存システムであって、前記データ保存装置に固有の秘密情報を格納する格納手段と、この格納手段に格納された秘密情報と、保存すべきデータとを用いて所定の処理を行うことにより前記保存すべきデータの改竄防止用データを生成する生成手段と、前記保存すべきデータと前記改竄防止用データとを対応させて前記保存媒体に記録する第1の記録手段と、前記保存媒体に予め記録されている媒体管理用データファイルに、前

記改竄防止用データを、前記保存すべきデータのファイルを識別する情報と対応させて記録する第2の記録手段と、前記格納手段に格納されている秘密情報と、前記媒体管理用データファイルを用いて所定の処理を行うことにより、前記媒体管理用データファイルの改竄防止用データを生成し、この改竄防止用データと前記媒体管理用データファイルとを対応させて、前記保存媒体に記録する第3の記録手段とを具備する。

【0009】また、第2の発明は、第1の発明において、前記媒体管理用データファイルには、前記保存媒体上に記録されている複数のデータファイルの改竄防止用データを、各々ファイルを識別する情報と対応させて記録する。

【0010】また、第3の発明は、第2の発明において、前記格納手段は改竄検知情報を格納しており、この改竄検知情報と、前記保存媒体に記録されている媒体管理用データファイルと、前記媒体管理用データファイルの改竄防止用データとを用いて所定の処理を行うことによつて、前記媒体管理用データファイルが改竄されているか否かを検知する第1の検知手段と、前記媒体管理用データファイルに登録されているファイルが全て、前記保存媒体上に存在しているか否かを確認する確認手段と、前記媒体管理用データファイルのレコードに登録されているデータファイルの改竄防止用データと、保存媒体上に前記データファイルと対応させて記録されている前記データファイルの改竄防止用データとが一致するかどうかを検知する第2の検知手段と、前記格納手段に格納されている改竄検知情報と、前記保存媒体に保存された前記保存すべきデータと、対応する前記改竄防止用データとを用いて所定の処理を行うことによつて、前記保存すべきデータが改竄されているか否かを検知する第3の検知手段とを具備する。

【0011】また、第4の発明は、第1～第3のいずれか1つの発明において、前記保存すべきデータは、通信回線を介して外部装置から送られてきたデータか、あるいは、前記データ保存装置のデータ入力機能を用いて入力されたデータである。

【0012】また、第5の発明は、第3または第4の発明において、前記保存媒体を初期化する時、あるいは初めてファイルを記録するときに、前記媒体管理用データファイルを前記保存媒体に記録する手段を有する。

【0013】また、第6の発明は、第3または第4の発明において、前記ファイル管理機能は、前記保存媒体上のデータファイルを削除する時に、前記媒体管理用データファイルから消去するデータファイルのレコードも削除する機能を持つ。

【0014】また、第7の発明は、第1～第6のいずれか1つの発明において、前記保存媒体は、前記データ保存装置に着脱自在な可搬型保存媒体か、あるいは、前記データ保存装置内に配置された固定型保存媒体である。

## 【0015】

【発明の実施の形態】まず、図1及び図2を参照して本発明の実施形態の概略を説明する。本実施形態のデータ保存システムを用いて保存媒体にデータを記録するときには、まず、図1に示すように、データ保存装置内の秘密情報を用いてデータファイルから改竄防止用データ（ここでは電子署名）を作成し（ステップS1）、この作成した電子署名を当該データファイルと対応付けて可搬型保存媒体に記録する（ステップS2）。

【0016】次に、記録したデータファイルの改竄防止用データ（電子署名）をデータファイルの識別情報と共にレコードとして、可搬型保存媒体上の保存媒体管理用の管理ファイル（以下、媒体管理用データファイルと呼ぶ）に記録する（ステップS3）。

【0017】次に、上記媒体管理用データファイルに対しても改竄防止用データ（電子署名）を作成して（ステップS4）、可搬型保存媒体上に記録する（ステップS5）。

【0018】次に上記のようにして記録されたデータが不正な第三者によって改竄されたかどうかを検証する方法を図2を参照して説明する。改竄検証の要求があったときには、まず媒体管理用データファイルの改竄を検証する（ステップS10）。次に登録されている全てのデータファイルの存在を確認し（ステップS11）、媒体管理用データファイルのレコード中の改竄防止用データと、対応するデータファイルの改竄防止用データ（電子署名）とを比較する（ステップS12）。このようにして全てのデータファイルに対して改竄を検証する（ステップS13）。

【0019】すなわち、媒体管理用データファイルは、可搬型保存媒体に必ず1つずつ存在するはずなので、当該ファイルが存在しない場合には、可搬型保存媒体に対して不正な処理がなされたことを検知できる。また、媒体管理用データファイルの改竄防止用データ（電子署名）から、媒体管理用データが改竄されたことが検知された場合にも、可搬型保存媒体に何らかの不正な処理がなされたことを検知することができる。

【0020】また、媒体管理用データファイル中のレコードに記録されている改竄防止用データと対応するデータファイルの改竄防止用データが異なる場合には、不正な差し替えが行われたことが検知できる。

【0021】また、媒体管理用データファイル中のレコードに存在するファイルが、可搬型保存媒体上に存在しない場合には、不正な消去が行われたことが検知できる。また、データファイルと、このデータファイルの改竄防止用データを用いることで、通常の電子署名と同様の方法で、データファイルが改竄されているかどうかを調べることができる。この処理は、保存媒体上のすべてのデータファイルに対して行なう。

【0022】以下に、上記した概略を後述する第1～第

3実施形態によりさらに詳細に説明する。ここでは改竄防止用データとして電子署名を用いた場合について説明するが、データの改竄を検知できるコードであるならば電子署名以外のコードであってもよいことは勿論である。

【0023】図3は本発明の第1実施形態に係るデータ保存システムの構成を示す図であり、データ保存装置30と、このデータ保存装置30に着脱自在な可搬型保存媒体2とからなり、保存すべきデータは通信回線3を介してホストコンピュータ1から供給される。データ保存装置30としては、ハードウェア的にはコンピュータの本体部分だけを使い、本体外壁を強固にパッケージ化したような構成を用いる。また、可搬型保存媒体2としては、光ディスクや可搬型ハードディスク、DAT、PCMCIAカード型メモリ、コンパクトフラッシュメモリなどの汎用の記録媒体を用いる。同様に、記録媒体を駆動する装置としても汎用の媒体駆動装置が用いられる。

【0024】図3に示すように、データ保存装置30は、通信回線3に接続可能な通信ポート11と、コマンド処理部12と、CPU21と、CPU作業用メモリ22と、プログラム格納用ROM23と、暗号鍵格納用メモリ24と、ファイル管理部25と、暗号・復号処理部26と、可搬型保存媒体2を駆動可能な可搬型保存媒体駆動装置27とを備えている。

【0025】また、本実施形態では、ユーザは他のパソコン等の情報機器（図1ではホストコンピュータ1）から通信回路3を通してしか、データ保存装置30及び可搬型保存媒体2内のデータにアクセスできないようになっている。つまり、ユーザがデータ保存装置30にデータを保存するためには、ホストコンピュータ1から、コマンド、データ及び必要な各種属性値を通信回線3を通してデータ保存装置30へ送る。データ保存装置30側では、受け取ったコマンドが正当な処理要求である場合にのみ保存の処理を行う。このような、従来のデータ保存システムとしては、原本性保証電子保存システム

（“原本性保証電子保存システムの開発—システムの構築”、MEDICAL IMAGING TECHNOLOGY, Vol. 16 NO. 4, p401-402, July 1998）がある。

【0026】まず、可搬型保存媒体2を初期化する方法を説明する。ここで説明する初期化の方法は後述する第2、第3実施形態に対しても同様に適用することができる。まず、ファイル管理部25の機能を用いて、可搬型保存媒体2にファイルが含まれているかどうかを調べる。ファイルが可搬型保存媒体2中に存在する場合には、初期化の処理は行わない。可搬型保存媒体2上にファイルが存在しない場合には、以下の手順で可搬型保存媒体2を初期化する。

【0027】可搬型保存媒体2に対して必要に応じて論理フォーマットを施す。その後、可搬型保存媒体2上に

媒体管理用データファイルを生成する。初期化時には媒体管理用データファイルに、データを初期化した時間や初期化したユーザに関する情報などを書き込む。次に、暗号鍵格納用メモリ24から電子署名作成用の暗号鍵データを読み出し、媒体管理用データファイルのデータと読み出した暗号鍵データから暗号・復号処理部26の機能を用いて改竄防止用データとしてデータ保存装置30の電子署名のデータを求めて、媒体管理用データファイルと対応づけて可搬型保存媒体2上に保存する。

【0028】次に、第1実施形態におけるデータ保存方法を説明する。データを保存するときには、ホストコンピュータ1から通信回線3を通してデータを保存するためのコマンド、データ及び必要な各種属性値を受け取る。ここで、各種属性とは、ファイル名、ユーザのアカウント名、ファイルサイズ、ファイル生成時刻等のファイル属性値などがある。次に、暗号鍵格納用メモリ24から電子署名作成用の暗号鍵データを読み出し、前記暗号鍵データと上記データから暗号・復号処理部26の機能を用いて改竄防止用データとしてデータ保存装置30の電子署名を求めて、データファイルと対応付けて保存する。

【0029】図4は可搬型保存媒体2に、保存するデータ1のファイル101と、データ1の電子署名102を対応付けて記録した状態を示している。その他のデータがある場合にはデータ2、データ3、…が電子署名2、3、…とそれぞれ対応付けて記録される。

【0030】次に、データ保存装置30の電子署名のデータを、保存すべきデータファイルのファイル名などのファイル識別子とともに、媒体管理用データファイル103中にレコードとして保存する。

【0031】図4は可搬型保存媒体2の媒体管理用データファイル103に、識別子1と電子署名1とを対応付けてデータファイル1のレコード105として記録した状態を示している。データ2、3、…がある場合には識別子2、3、…と電子署名2、3、…とが対応付けて記録される。

【0032】その後、この媒体管理用データファイル103が改竄されないように、前記暗号鍵データを用いて媒体管理用データファイル103から、暗号・復号処理部26の機能を用いて媒体管理用データファイル103に対する改竄防止用コードであるデータ保存装置30の電子署名104を求め、媒体管理用データファイル103と対応させて可搬型保存媒体2上に保存する。なお、図中には示していないが媒体管理用データファイル103内には、前述した保存媒体初期化時の初期化データも記録されている。図4は可搬型保存媒体2上に媒体管理用データファイル103の電子署名104を記録した状態を示している。

【0033】図5は本発明の第2実施形態に係るデータ保存システムの構成を示す図であり、データ保存装置と

して、デジタルカメラのような画像入力装置を用いた場合の例である。図中、図3と同じ番号のモジュールは図3と同じ機能を果たすことを意味する。

【0034】データは、画像撮像部30にて図示していないレンズ系、CCD素子、A/D変換器、ファイルフォーマット作成部等を経て、画像データとしてCPU作業用メモリ22に蓄積される。その後、ユーザがデジタルカメラ40のユーザインタフェース29を通して、上記画像データを保存するという指示をデジタルカメラ40に送ると、暗号鍵格納用メモリ24から電子署名作成用の暗号鍵データを読み出し、暗号鍵と上記データから暗号・復号処理部26の機能を用いて改竄防止用データとして電子署名を求めて、図4に示すようにデータファイル101と対応付けて保存する。

【0035】さらに、この時に電子署名のデータを、保存するデータファイルのファイル名などのファイル識別子とともに媒体管理用データファイル103中にレコード105として保存する。その後、この媒体管理用データファイル103が改竄されないように、前記暗号鍵データと媒体管理用データファイル103から、暗号・復号処理部26の機能を用いて媒体管理用データファイル103の電子署名を求め、媒体管理用データファイル103と対応させて可搬型保存媒体2上に保存する。

【0036】図6は本発明の第3実施形態に係るデータ保存システムの構成を示す図であり、データ保存装置としてデジタル録音機のような音声入力装置を用いた場合の例である。図中、図3と同じ番号のモジュールは図3と同じ機能を果たすことを意味する。

【0037】データは、音声入力部50にて図示していないマイク、A/D変換器、ファイルフォーマット作成部等を経て、音声データとしてCPU作業用メモリ22に蓄積される。その後、ユーザがデジタル録音機60のユーザインタフェース29を通して、上記音声データを保存するというコマンドを入力すると、暗号鍵格納用メモリ24から電子署名作成用の暗号鍵データを読み出し、暗号鍵と上記データから暗号・復号処理部26の機能を用いて改竄防止用データとして電子署名を求めて、図4に示すようにデータファイル101と対応付けて保存する。

【0038】さらに、この時に電子署名のデータを媒体管理用データファイル103中に、保存するデータファイルのファイル名などのファイル識別子とともにレコード105として保存する。その後、この媒体管理用データファイル103自体が改竄されないように、前記暗号鍵データと媒体管理用データファイル103のデータから、暗号・復号処理部26の機能を用いて媒体管理用データファイル103の電子署名104を求め、媒体管理用データファイル103と対応させて可搬型保存媒体2上に保存する。

【0039】次に、本実施形態のデータ保存システムを

用いて可搬型保存媒体 2 からデータファイルを正規の手続きで消去する方法について説明する。第 1 実施形態の場合は、ホストコンピュータ 1 から送られてきたデータファイルを消去するコマンドに応じて、可搬型保存媒体 2 上の指定されたファイルを消去する。第 2、第 3 実施形態の場合には、ユーザインタフェース 29 を用いてユーザが入力したデータファイル消去要求に応じて、可搬型保存媒体 2 上の指定されたファイルを消去する。

【0040】データファイルを可搬型保存媒体 2 から消去する場合には、同時に媒体管理用データファイル 103 上の消去するデータファイルのレコードも削除する。その後、暗号鍵格納用メモリ 24 から電子署名作成用の暗号鍵データを読み出し、媒体管理用データファイル 103 と暗号鍵データから暗号・復号処理部 26 の機能を用いて改竄防止用データとしてデータ保存装置の電子署名 104 のデータを作成しなおし、媒体管理用データファイル 103 と対応づけて可搬型保存媒体 2 上に上書きにより保存する。

【0041】なお、レコードの削除は、媒体管理用データファイル 103 から実際に削除しても良いし、また、各レコードの先頭などに削除されたかどうかを示すフラグを設け、例えばそのレコードが存在するなら対応するフラグを 1 に、削除されたなら 0 にすることで、媒体管理用データファイル 103 からレコードを削除したことにより（後者を仮削除と呼ぶ）。なお、仮削除をする場合には、媒体管理用データファイル 103 に対応する電子署名 104 を作成する際にフラグの情報も含める。

【0042】次に、本実施形態のデータ保存システムを用いて可搬型保存媒体 2 からデータファイルの識別子を正規の手続きで変更する手法について説明する。ファイル名の変更、ディレクトリの変更等、ファイル識別子を変更する場合には、同時に媒体管理用データファイル 103 上の対応するレコードのファイル識別子をも変更する。その後、暗号鍵格納用メモリ 24 から電子署名作成用の暗号鍵データを読み出し、媒体管理用データファイル 103 と暗号鍵データから暗号・復号処理部 26 の機能を用いて改竄防止用データとしてデータ保存装置 30 の電子署名のデータを作成しなおし、媒体管理用データファイル 103 と対応づけて可搬型保存媒体 2 上に上書きにより保存する。

【0043】次に、第 1 実施形態の方法を用いて本実施形態のデータ保存システムの不正な消去を含むデータの改竄検知の方法を説明する。改竄検知の方法は、基本的に第 2、第 3 実施形態においても同様である。第 1 実施形態の場合と異なる処理を行う必要のある部分については個々に説明する。

【0044】まず、可搬型保存媒体 2 上のデータファイルの改竄を検知するために、各々のデータファイル（媒体管理用データファイルを含む）のデータ及び、対応す

る電子署名と暗号鍵格納用メモリ 24 から読み出した改竄検知用データとしての復号用の鍵から、暗号・復号処理部 26 の機能を用いて個々のファイルの改竄検知を行う。改竄の有無を検知するには、まず、検知するデータに所定の処理を施してメッセージ・ダイジェストと呼ばれるコード（コード 1 と呼ぶ）を抽出する。また、データファイルの電子署名データを、暗号鍵格納用メモリ 24 から読み出した復号用の鍵を用いて復号してコード（コード 2 と呼ぶ）を取り出す。

【0045】その後、前記所定の処理を施して得られたコード 1 と前記電子署名を復号化して得たコード 2 とを比較し、両者が一致している場合には改竄されていない、一致していない場合にはデータファイルが改竄されていると判断することで改竄検知の処理を行う。改竄されている場合には、第 1 実施形態の場合には通信回路 3 を介してホストコンピュータ 1 側に、第 2、第 3 実施形態の場合にはユーザインタフェース 29 を介してユーザに改竄があったことを通知する。

【0046】また、可搬型保存媒体 2 上のデータファイルの不正な消去を検知するには、ファイル管理部 25 の機能を用いて媒体管理用データファイル 103 にレコードとして登録されているファイルが、すべて可搬型保存媒体 2 上に存在するかどうかを調べる。もし、ファイルが一つでも存在しない場合には、データファイルが不正に消去させていることになる。不正な消去があった場合には、第 1 実施形態の場合には通信回路 3 を介してホストコンピュータ 1 側に、第 2、第 3 実施形態の場合にはユーザインタフェース 29 を介してユーザに不正にデータが消去されたことを通知する。

【0047】また、可搬型保存媒体 2 上のデータファイルの不正な差し替えを検知するには、ファイル管理部 25 の機能を用いて、保存されている全てのデータファイルの電子署名と媒体管理用データファイル 103 の対応するレコードに記録されている電子署名とを照合する。一致しないデータファイルがある場合には、そのファイルは不正に差し替えられたことになる。不正な差し替えがあった場合には、第 1 実施形態の場合には通信回路 3 を介してホストコンピュータ 1 側に、第 2、第 3 実施形態の場合にはユーザインタフェース 29 を介してユーザに不正にデータが消去されたことを通知する。

【0048】また、上記の処理を行っているときに、媒体管理用データファイル 103 にレコードが登録されていないファイルが可搬型保存媒体 2 上に存在した場合には、本実施形態のデータ保存システム以外のシステムを用いてデータファイルが保存されたことになり、この場合にも不正があったとして、第 1 実施形態の場合には通信回路 3 を介してホストコンピュータ 1 側に、第 2、第 3 実施形態の場合にはユーザインタフェース 29 を介してユーザに不正にデータが保存されていることを通知する。



【0049】さらに、改竄防止用データ作成及び改竄検知の手段として、公開鍵暗号方式のように、改竄防止用データ作成時と改竄検知時で用いる情報（鍵）が異なるものを用いた場合、改竄防止用データ作成のための情報だけをデータ保存装置内に安全に格納すればよいので、改竄検知用の情報を公開することでデータ保存装置以外の汎用の装置でも改竄検知の処理を行うことができる。

【0050】なお、上記実施形態中では媒体管理データのレコード中には、データファイルの識別子とデータファイルの電子署名を記録するとししか記述しなかったが、ファイルに関する他の情報等をレコードの属性中に定義しても構わない。例えば、媒体管理データ中のレコードを検索で使えるようにするためにレコード中に、キーワードを含めるといった構成も考えられる。

【0051】また、媒体管理用データファイルとして、可搬型保存媒体2上の全てのファイルをまとめて1つのファイルとしたものを用いても、（このファイルを媒体管理用データファイル'と呼ぶ）、改竄検知に関しては同様の効果は得られる。しかし、この場合には媒体管理用データファイル'のサイズが非常に大きくなり、電子署名104を作成するために処理時間が非常に長くなってしまふ。しかも、電子署名104は可搬型保存媒体上のどのファイルを更新しても、必ず更新される必要があるため非常に効率の悪いデータ保存システムになってしまう。

【0052】一方、本実施形態で提案した手法では媒体管理用データファイルに記録されるデータは、前記媒体管理用データファイル'に比べ非常に小さくなる。媒体管理用データファイルのレコードのサイズは、ファイルの識別子とファイルに対応した電子署名のサイズの合計なのでせいぜい数百バイトであり、一方、通常のファイルのサイズは、数十キロ〜数メガバイトである。したがって、媒体管理用データファイルは媒体管理用データファイル'に比べて1/100〜1/10000程度小さくなる。そのため、提案した手法を用いることで電子署名104を更新するための処理時間は短くなる。

【0053】以上、上記した実施形態を要約すると以下のようになる。すなわち、データ保存システムを用いてデータファイルを保存するときには、データファイルの改竄防止用データ（電子署名）を作成して、データファイルと対応付けて可搬型保存媒体2上に保存するとともに、媒体管理用データファイル103にデータファイルの識別子と前記改竄防止用データをレコードとして記録し、さらに、媒体管理用データファイル103の改竄防止用データを作成して、可搬型保存媒体2上に保存する。

【0054】また、データ保存システムを用いて改竄を検知するときには、前記媒体管理用データファイル103と媒体管理用データファイル103の改竄防止用データ104を用いて改竄の有無を検証する。さらに、媒体

管理用データファイル103のレコードに登録されているデータファイルが全て可搬型保存媒体2上に存在するかどうかを確認し、不正な消去が行われなかったか確認する。また、データファイルの改竄防止用データと、媒体管理用データファイル103のレコードに記録されているデータファイルの改竄防止用データを照合し、一致しているかどうかを調べることで、データファイルの不正な差し替えがなかったか否かを確認する。その後、可搬型保存媒体2上の各データファイルと対応する改竄防止用データを用いてデータファイルの改竄の有無を検証する。

【0055】以上の処理において、不正を検知した場合には通信回線3、もしくはインタフェース29を用いてユーザに不正があったことを通知する。上記した実施形態によれば、データ保存装置以外には、可搬型保存媒体2にデータを保存するときに作成する改竄防止用データを作成できないようにすることが可能となる。また、可搬型保存媒体2に保存される全てのファイルの改竄防止用データは、可搬型保存媒体2上の媒体管理用データファイル103に登録され、媒体管理用データファイル103自体にも改竄防止用データが付けられる。以上の処理を行うことで、データファイルの不正消去、不正コピーを含む可搬型保存媒体2上のファイルの改竄を防止することが可能となる。

【0056】つまり、データファイルの改竄防止用データを調べることで、データファイルが本実施形態の保存システム以外のシステムを用いて不正に改竄されたかどうかを検知できる。また、媒体管理用データファイル103に登録されている改竄防止用データと、対応するデータファイルの改竄防止用データを比較することで、本実施形態の保存システム以外のシステムを用いて不正にデータファイルが消去、あるいはコピーされたかどうかを検知できる。このようにして、汎用の可搬型保存媒体を用いても、データファイルの不正な消去、コピーを含む改竄を防止できる。

【0057】なお、上記した実施形態ではデータ保存装置に着脱自在な可搬型保存媒体を用いたが、データ保存装置内に配置された固定型保存媒体を用いるようにしてもよい。

#### 【図面の簡単な説明】

【図1】本発明の実施形態に係るデータ保存方法を説明するためのフローチャートである。

【図2】記録されたデータが不正な第三者によって改竄されたかどうかを検証する方法を説明するためのフローチャートである。

【図3】本発明の第1実施形態に係るデータ保存システムの構成を示す図である。

【図4】可搬型保存媒体に本実施形態の方法によりデータファイルを保存した状態を示す図である。

【図5】本発明の第2実施形態に係るデータ保存システ

13

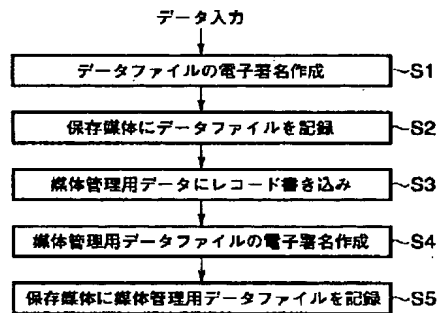
ムの構成を示す図である。

【図6】本発明の第3実施形態に係るデータ保存システムの構成を示す図である。

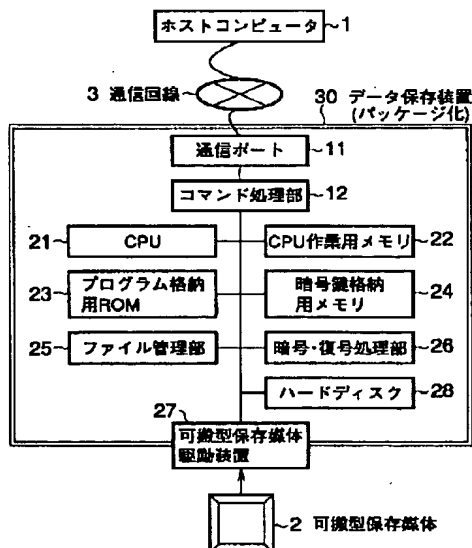
【符号の説明】

- 1…ホストコンピュータ、  
2…可搬型保存媒体、  
3…通信回線、  
11…通信ポート、  
12…コマンド処理部、  
21…CPU、  
22…CPU作業用メモリ、

【図1】



【図3】



14

23…プログラム格納用ROM、

24…暗号鍵格納用メモリ、

25…ファイル管理部、

26…暗号・復号処理部、

27…可搬型保存媒体駆動装置、

28…ハードディスク、

101…保存するデータ1のファイル、

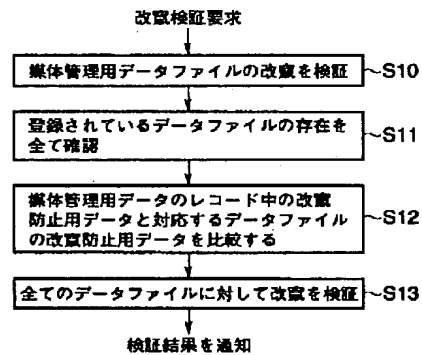
102…データ1の電子署名、

103…媒体管理用データファイル、

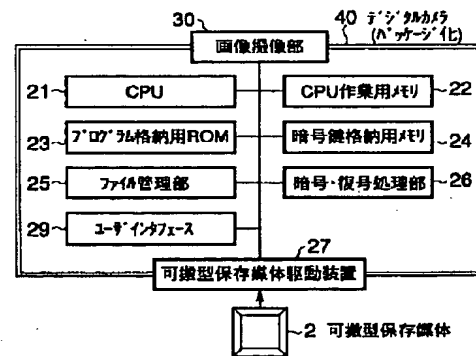
104…媒体管理用データファイルの電子署名、

105…データファイル1のレコード。

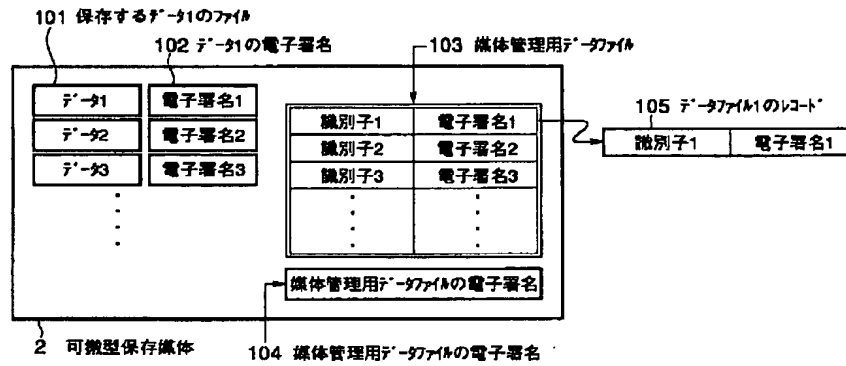
【図2】



【図5】



【図 4】



【図 6】

